جامعة بيرزيت

BIRZEIT UNIVERSITY

Secure Software Development (SWEN7302)
Dr: Ahmad Alsadeh

Homework Assignment #2

By Hanan Namrouti(1165217)

1. A static analysis

- **analyzes a program's code without running it**

2. Which of the following are advantages of static analysis over testing??

- **A static analysis can reason about all program paths, not just some of them**

3. Which of the following are not the advantages of static analysis over testing?

- **Many other program analysis problems can be converted to the halting problem.**

4. . Suppose we have a static analysis that aims to find buffer overflows in C programs. If the analysis is sound, then which of the following is true about it?

- **It may have false alarms, but will not fail to report actual bugs**

5. A tainted flow is?

- **A flow from an untrusted source to both trusted and untrusted sinks**

6. Consider the program below, using the qualified types annotations for tainted flows given in the lecture (shown in comments). In particular, notice that the variable fmt and the argument to printf are untainted, while the result of fgets is tainted. Suppose we analyze this with a tainted flow analysis. This program has no bugs, but which kinds of analysis report a false alarm?

- **flow-sensitive, context-sensitive**

7.Consider the following code, where the referenced chomp function is the same as in the previous question. Suppose we analyze this with a tainted flow analysis. Once again, this program has no bugs, but which kinds of analysis report a false alarm??

- **An actor, or role, that is the subject of a security policy: Principals can be people, computer programs, or some other entity acting in a particular role, like manager or client**

8.Consider the following code, where the referenced chomp function is the same as in the previous question. Suppose we analyze this with a tainted flow analysis. Once again, this program has no bugs, but which kinds of analysis report a false alarm?

- NONE

9.Which of the following are true of implicit flows??

- **One can occur when assigning an untainted value to an untainted variable, but conditioned on a tainted value**
- **Implicit flows are rarely detected by tainted flow analyses, because detecting them can increase false alarms**

10. What is a key advantage of symbolic execution over static analysis?

- **As a generalized form of testing, when a symbolic executor finds a bug, we are sure it is not a false alarm**
- **Moreover, one can often produce a test case from the alarm that reproduces the bug, making it easier to fix**

11.Symbolic execution, viewed as a kind of static analysis, has which of the following "sensitivities?"

- **Flow-sensitivity**
- **Context-sensitivity**
- **Path-sensitivity**

12. . Why is concolic execution problematic for non-terminating programs??

- **Its search strategy is to choose new test cases based on constraints generated by terminating runs**
- **As such, a non-terminating program may not produce a terminating test, and thus will never produce constraints to produce the next test.**

13.Suppose that x and y in the following program are symbolic. When the symbolic executor reaches the line that prints "everywhere" what will the path condition be??

- **$x > 5 \wedge \neg(y > 7) \wedge x < 20$**

14. Suppose that x in the following program is symbolic. When the symbolic executor reaches the line that prints "here" what will the path condition be??

- **x > 5**

15. Which of the following are heuristics that symbolic executors use to cover more of the search space?

- **Randomly restart the search from the main function**
    - **This avoids the problem of being stuck in a "local minimum", i.e., a portion of the program that has many paths, at the expense of exploring other parts of the program**
- **Choose between two paths based on whether one reaches program statements not previously executed**
    - **This approach intends to maximize "coverage" under the theory that executing all lines of code is more important than executing arbitrary groups of paths in the same code area**
- **Choose between two paths based on a notion of priority**
    - **Coverage is one kind of priority; another kind might be based on whether some other static analysis tool finds part of the path suspicious**